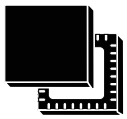
ST33KTPM2XSPI ST33KTPM2XI2C

Data brief

TPM 2.0 devices with an SPI or I²C interface



UFQFPN32 (5 × 5 × 0.55 mm)

Features

TPM features

- Flash-memory-based trusted platform module (TPM)
- Compliant with Trusted Computing Group (TCG) trusted platform module (TPM) Library specifications 2.0, revision 1.59 errata version 1.3 and TCG PC Client Platform TPM Profile (PTP) for TPM 2.0 Version 1.05
- Fault-tolerant firmware loader that keeps the TPM fully functional when the loading process is interrupted (self-recovery)
- SP800-193 compliant for protection, detection and recovery requirements
- Targeted certifications:
  - Common Criteria in compliance with the TPM 2.0 protection profile (augmented with AVA_VAN.5, resistant to high-potential attacks)
  - FIPS 140-3
  - TCG certification
- SPI support at up to 66 MHz
- I²C communication bus running at up to 1 Mb/s

Hardware features

- Highly reliable flash memory with error correction code
- Extended temperature range: −40 °C to 105 °C
- ESD (electrostatic discharge) protection up to 4 kV (HBM)
- 1.8 V or 3.3 V supply voltage range

Security features

- Active shield
- Monitoring of environmental parameters
- Hardware and software protection against fault injection
- FIPS SP800-90A and AIS20-compliant deterministic random-bit generator (DRBG)
- FIPS SP800-90B and AIS31-compliant true random-number generator (TRNG)
- Cryptographic algorithms:
  - RSA key generation (1024, 2048, 3072 and 4096 bits)
  - RSA signature (RSASSA-PSS, RSASSA-PKCS1v1_5)
  - RSA encryption (RSAES-OAEP, RSAESPKCS1-v1_5)
  - SHA-1, SHA-2 (256 and 384 bits), SHA-3 (256 and 384 bits)
  - HMAC SHA-1, SHA-2 and SHA-3
  - AES-128,192 and 256 bits
  - ECC (NIST P-256, P-384 curves): key generation, ECDH and ECDSA, ECSchnorr
  - ECDAA (BN-256 curve)
- Device provided with 3 endorsement keys (EK) and EK certificates (RSA2048, ECC NIST P_256 and ECC NIST P_384)
- Device provisioned with three 2048-bit RSA key pairs to reduce the TPM provisioning time

Product's targeted compliance

- Compliant with Microsoftt ® Windows® 10 and 11
- Compliant with Linux® drivers
- Compliant with Intel® vPro® technology
- Compliant with TCG test suite for TPM 2.0
- Compliant with the open-source TCG TPM 2.0 TSS implementation

1 Description

The STSAFE-TPM (trusted platform module) family of products offers a broad portfolio of standardized solutions for embedded, PC, mobile, and computing applications.

It includes turnkey products compliant with the Trusted Computing Group (TCG) standards that provide services to protect the confidentiality, integrity, and authenticity of information and devices.

The STSAFE-TPM devices are easy to integrate thanks to the variety of supported interfaces and the availability of TPM ecosystem software solutions.

They target Common Criteria, TCG, and FIPS certification.

The ST33KTPM2XSPI offers a slave serial peripheral interface (SPI) by default whereas the ST33KTPM2XI2C offers exclusively a slave SPI or a slave I²C interface. Both devices are compliant with the TCG *PC Client TPM Profile* specifications.

It offers resilience services during the TPM firmware upgrade process, and self-recovery of TPM firmware and critical data upon failure detection.

The ST33KTPM2XSPI and ST33KTPM2XI2C operate in the –40 °C to 105 °C extended temperature range.

The device is offered in the UFQFPN32 ECOPACK2 package. ECOPACK is an ST trademark.

2 UFQFPN32 pin and signal description

The figure below gives the pinout of the UFQFPN32 package in which the devices are delivered. Table 1 describes the associated signals.

Figure 1. UFQFPN32 pinout

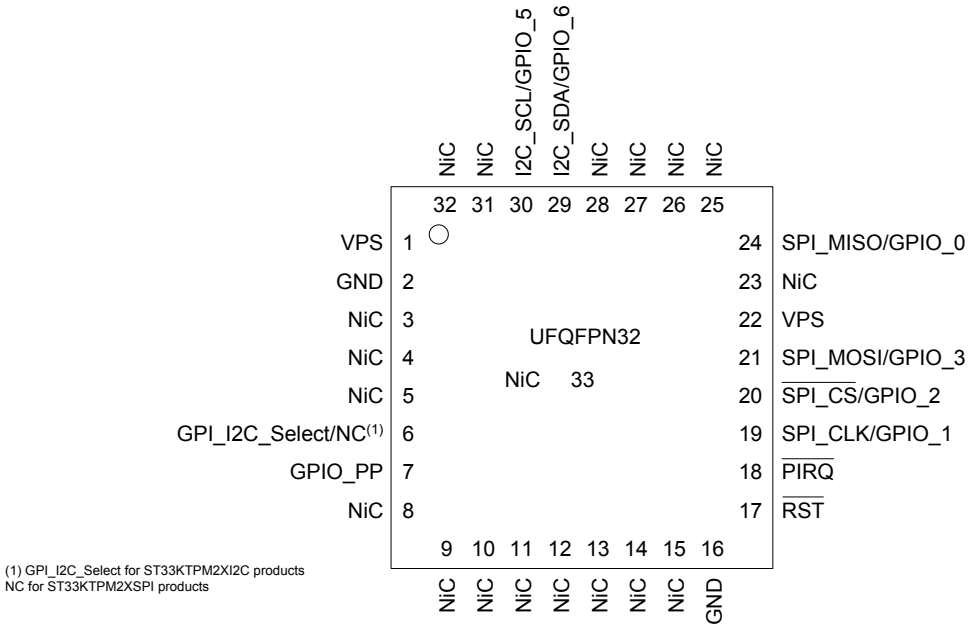


Table 1. UFQFPN32 descriptions

Signal	Type	Description
VPS	Input	**Power supply**. This pin must be connected to 1.8 V or 3.3 V DC power rail supplied by the motherboard.
GND	Input	**Ground**, has to be connected to the main motherboard ground.
$\overline{RST}$	Input	**Reset**, active low, used to re-initialize the device. Must not be unconnected. External pull-up resistor required if it cannot be driven.
SPI_MISO/GPIO_0	Output(1)	**SPI master input, slave output** (output from slave) / General-purpose input/output if I^2C is activated
SPI_MOSI/GPIO_3	Input(1)	**SPI master output, slave input** (output from master) / General-purpose input/output if I^2C is activated
SPI_CLK/GPIO_1	Input(1)	**SPI serial clock** (output from master) / General-purpose input/output if I^2C is activated
$\overline{SPI\_CS}$/GPIO_2	Input(1)	**SPI chip (or slave) select**, internal pull-up (active low; output from master) / General-purpose input/output if I^2C is activated
$\overline{PIRQ}$	Output	**IRQ**, active low, open drain, used by the TPM to generate an interrupt
GPIO_PP	Input	**Physical presence**, active high, internal pull-down. Used to indicate physical presence to the TPM.
GPI_I2C_Select	Input	This pin must be connected to an external pull-down resistor to activate the I²C protocol during product boot time. It can remain unconnected for the SPI protocol. This pin is internal pull-up by default and becomes internal floating after I²C activation.
NiC	-	**Not internally connected**: not connected to the die. May be left unconnected but no impact on TPM if connected.
NC	-	**Not connected**: connected to the die but unused. Must be left unconnected.
I2C_SDA/GPIO_6	Input/ output(1)	**Bidirectional I²C serial data** (open drain without a weak pull-up resistor) / General-purpose input/output if SPI is activated
I2C_SCL/GPIO_5	Input(1)	**Input I²C serial clock** (open drain without a weak pull-up resistor) / General-purpose input/output if SPI is activated

1. *In GPIO configuration, this signal is Input/output.*

Note: The UFQFPN32 package has a central pad (PIN33) on the bottom, which is not connected to the die. This pin does not impact the TPM, be it connected or not.

3 Electrical integration guidance

This section gives some guidance on how to integrate the ST33KTPM2XSPI or ST33KTPM2XI2C device in an application.

3.1 Recommended power supply filtering

The power supply of the device should be filtered using the circuit shown in the figure below.

Figure 2. Recommended filtering capacitors on V_{CC}

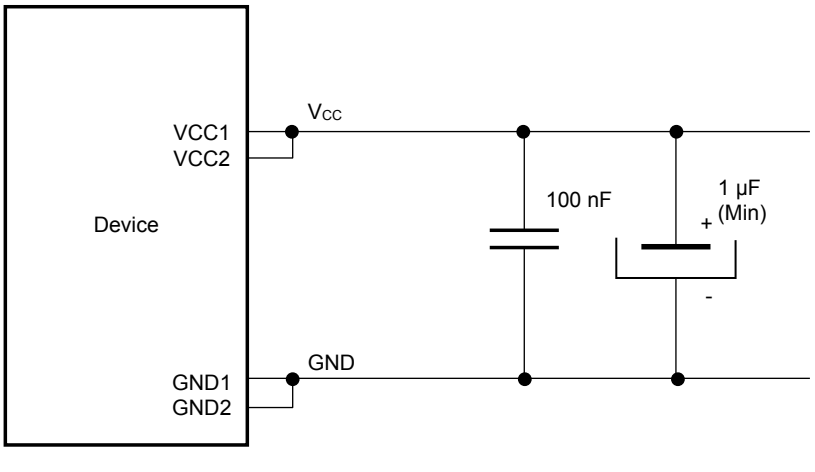


Table 2. V_{CC} rising slope

Symbol	Parameter	Min.	Typ.	Max.	Unit
S_{VCC}	V_{CC} rising slope	2	-	$2 \cdot 10^3$	V/ms

Note: Measurement must be done between 1.36 V and 1.62 V

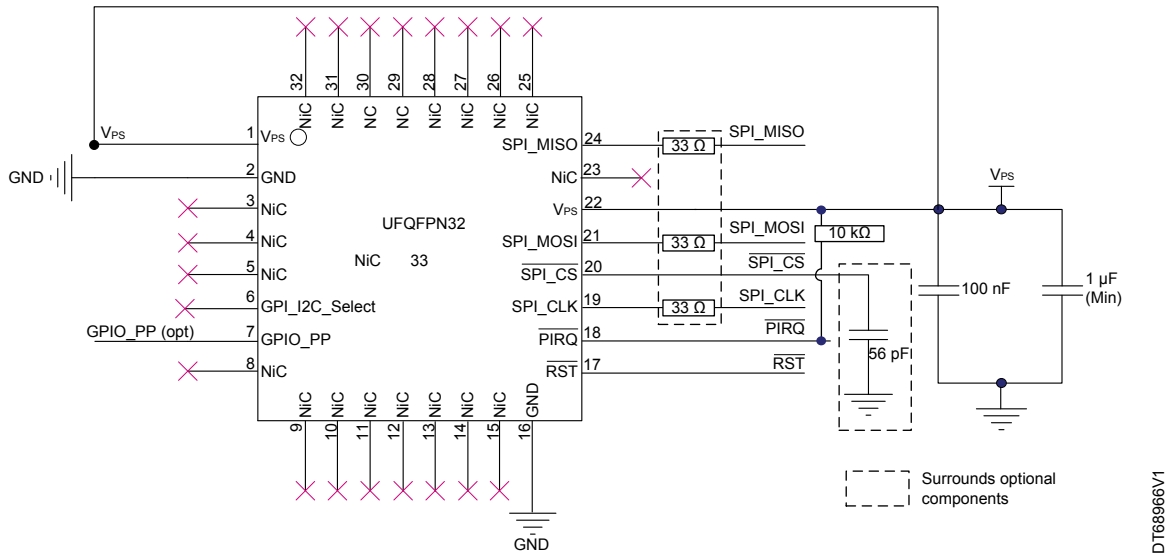
3.2 $\overline{\text{SPI\_CS}}$ optional filtering

Recommendation for SPI_CS integration: It is mandatory that SPI_CLK is at the low logic level when the falling edge occurs on the SPI_CS signal. An external capacitance of 56 pF is recommended on SPI_CS for that purpose. This capacitor might not be required depending on the intrinsic line capacitance, the SPI bus frequency, or both.

3.3 Device integration for SPI communication

The figure below shows the typical hardware implementation of the ST33KTPM2XSPI device for SPI communication.

Figure 3. Typical hardware implementation for SPI communication (UFQFPN32 package)



Note: The use of a low-value resistor (typically 33 Ω) on SPI_MISO, SPI_MOSI and SPI_CLK can be recommended for line adaptation when the signals are affected by parasite spikes. Its use is mandatory to avoid disturbance of the ramp-up and ramp-down signals.

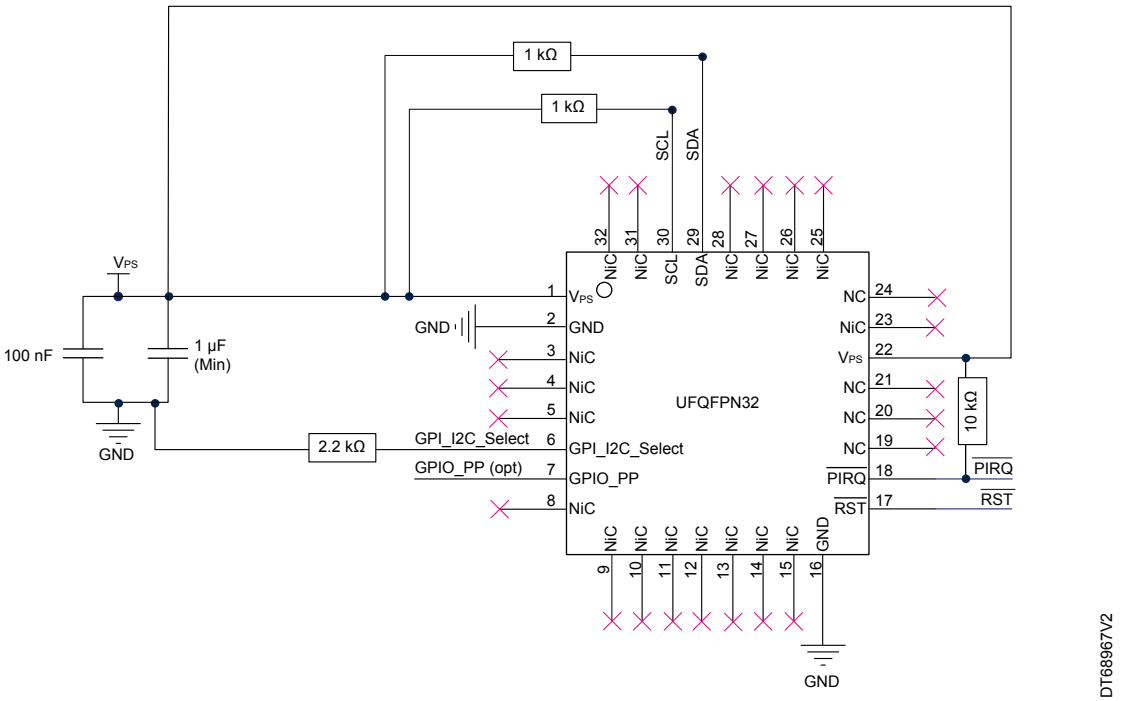
Note: The capacitor on $\overline{SPI\_CS}$ is optional (see Section 3.2 SPI_CS optional filtering).

Note: The pull-up resistor on the PIRQ line is mandatory to optimize the power consumption in standby mode.

3.4 Device integration for I²C communication

The figure below shows the typical hardware implementation of the ST33KTPM2XI2C device for I²C communication.

Figure 4. Typical hardware implementation for I²C communication (UFQFPN32 package)



Note: The pull-up resistor on the PIRQ line is mandatory to optimize the power consumption in standby mode.

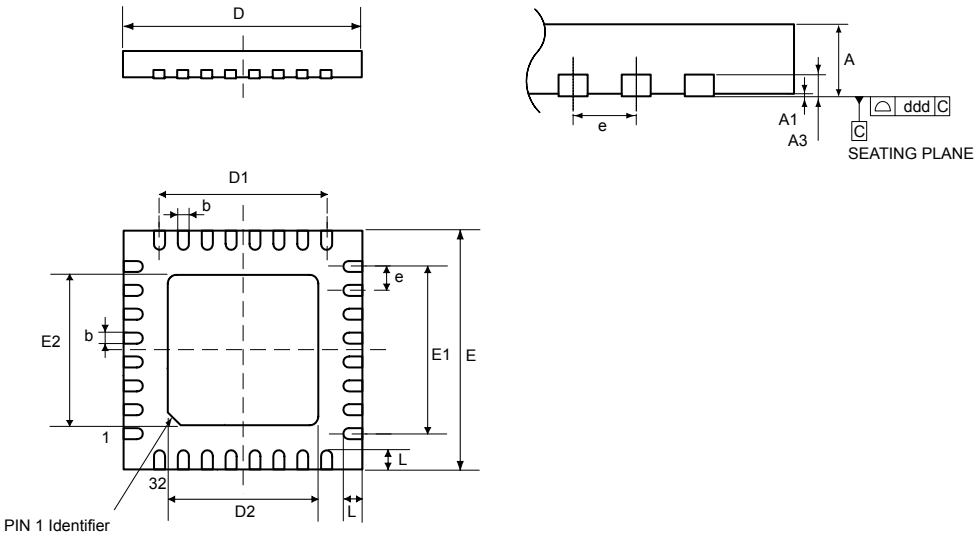
4 Package information

In order to meet environmental requirements, ST offers these devices in different grades of ECOPACK packages, depending on their level of environmental compliance. ECOPACK specifications, grade definitions and product status are available at: www.st.com. ECOPACK is an ST trademark.

4.1 UFQFPN32 package information

UFQFPN stands for 32-pin, 5 × 5 × 0.550 mm, 0.5 mm pitch, thermally enhanced, ultra-fine pitch, quad flat package, no lead.

Figure 5. UFQFPN32 - Outline



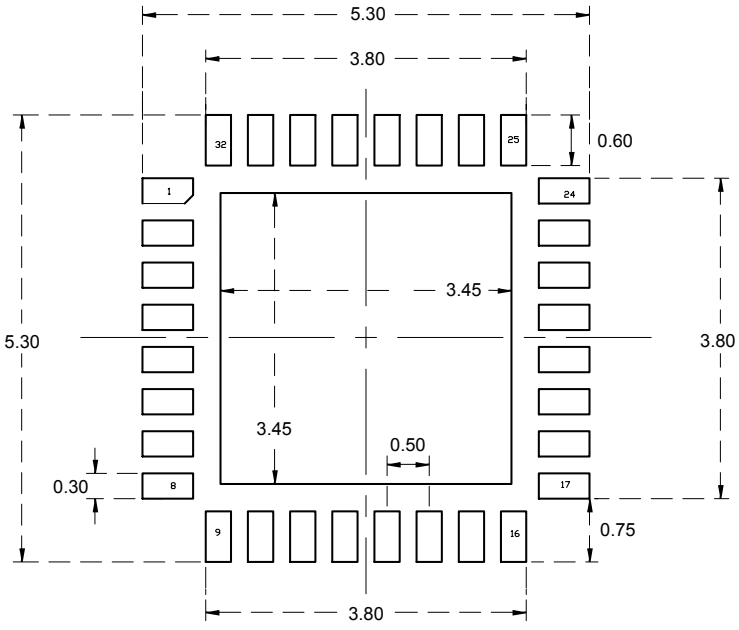
1. Drawing is not to scale.
2. All leads/pads should also be soldered to the PCB to improve the lead/pad solder joint life.
3. There is an exposed die pad on the underside of the UFQFPN package. It is recommended to connect and solder this backside pad to the PCB ground.

Table 3. UFQFPN32 - Mechanical data

Symbol	Millimeters			Inches[1]		
	Min	Typ	Max	Min	Typ	Max
A	0.500	0.550	0.600	0.0197	0.0217	0.0236
A1	0.000	0.020	0.050	0.0000	0.0008	0.0020
A3	-	0.152	-	-	0.0060	-
b	0.180	-	0.300	0.0071	-	0.0118
D[2]	4.900	5.000	5.100	0.1929	0.1969	0.2008
D1	3.400	-	3.700	0.1339	-	0.1457
D2	3.400	-	3.700	0.1339	-	0.1457
E[2]	4.900	5.000	5.100	0.1929	0.1969	0.2008
E1	3.400	-	3.700	0.1339	-	0.1457
E2	3.400	-	3.700	0.1339	-	0.1457
e	-	0.500	-	-	0.0197	-
L	0.300	0.400	0.500	0.0118	0.0157	0.0197
ddd	-	-	0.080	-	-	0.0031

1. *Values in inches are converted from mm and rounded to 4 decimal digits.*
2. *Dimensions D and E do not include mold protrusion, not to exceed 0.15 mm.*

Figure 6. UFQFPN32 - Recommended footprint



1. Dimensions are expressed in millimeters.

5 Delivery packing

Surface-mount packages can be supplied with tape and reel packing. The reels have a 13" typical diameter.

Reels are in plastic, either anti-static or conductive, with a black conductive cavity tape. The cover tape is transparent anti-static or conductive.

The devices are positioned in the cavities with the identifying pin (normally Pin “1”) on the same side as the sprocket holes in the tape.

The STMicroelectronics tape and reel specifications are compliant with the EIA 481-A standard specification.

Table 4. Packages on tape and reel

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
UFQFPN32	Very thin fine pitch quad flat pack no-lead package	12 mm	8 mm	13 in.	3000

Figure 7. Reel diagram

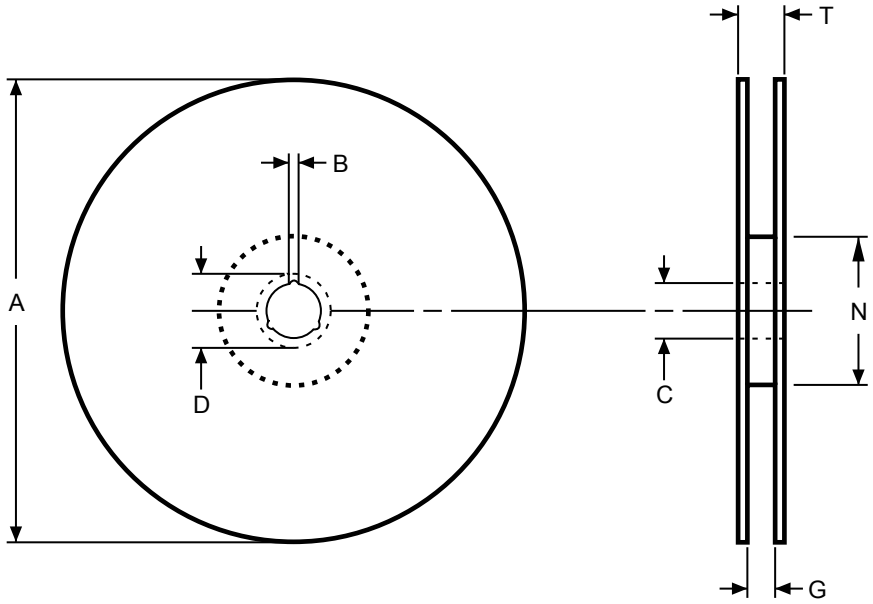
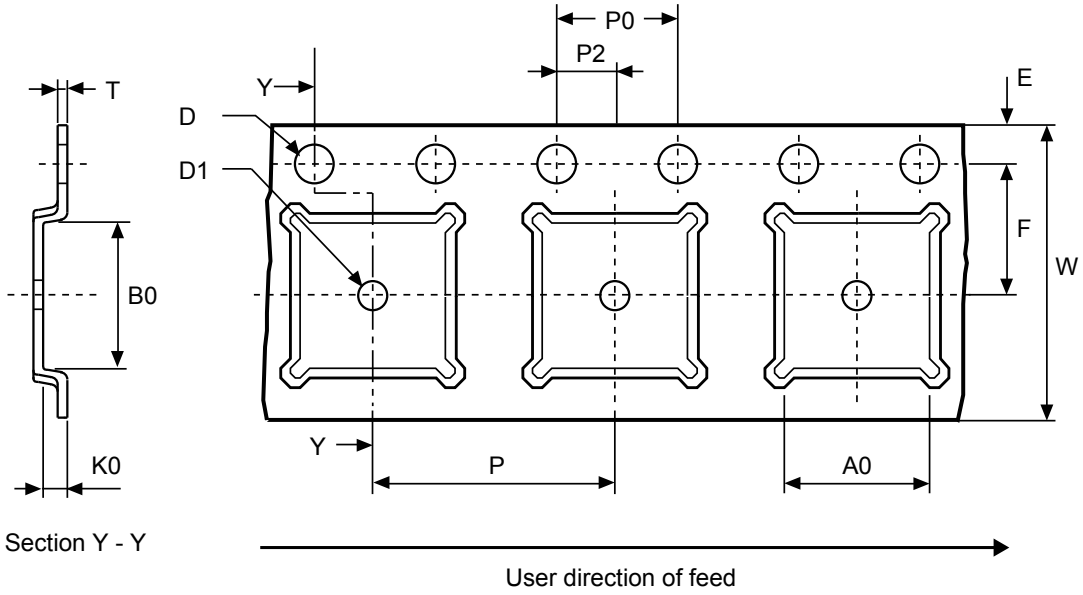


Table 5. Reel dimensions

Reel size	Tape width	A Max.	B Min.	C	D Min.	G Max.	N Min.	T Max.	Unit
13”	12	330	1.5	13 ±0.2	20.2	12.6	100	18.4	mm

Figure 8. **UFQFPN32 - Embossed carrier tape**



1. Drawing is not to scale.

Figure 9. **UFQFPN32 - Chip orientation in the embossed carrier tape**

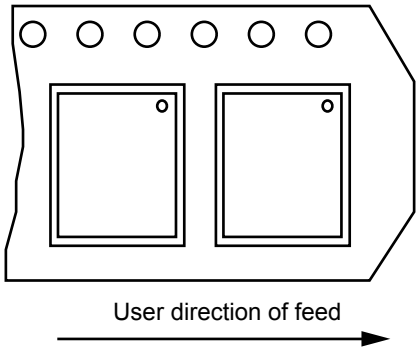


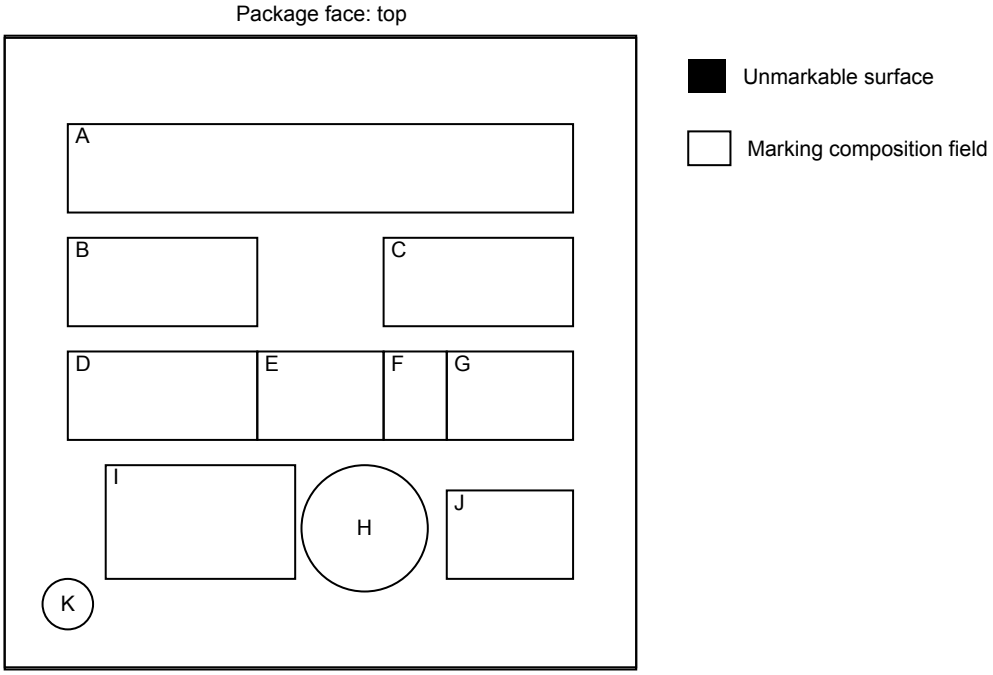
Table 6. **UFQFPN32 - Carrier tape dimensions**

Package	A0	B0	K0	D1 Min.	P	P2	D	P0	E	F	W	T Max.	Unit
UFQFPN 5×5	5.3 ±0.1	5.3 ±0.1	0.75 ±0.1	1.5	8 ±0.1	2 ±0.05	1.55 ±0.05	4 ±0.1	1.75 ±0.1	5.5 ±0.1	12 ±0.3	0.3 ±0.05	mm

6 UFQFPN32 package marking information

Parts marked as E or ES (for engineering sample) are not yet qualified and therefore not approved for use in production. ST is not responsible for any consequences resulting from such use. In no event will ST be liable for the customer using any of these engineering samples in production. ST's Quality department must be contacted prior to any decision to use these engineering samples to run a qualification activity.

Figure 10. UFQFPN32 standard marking example



Legend:

A: Marking area – 8 digits
B: Marking area – 3 digits
C: BE sequence (LLL)
D: Country of origin (3 characters allowed (max.))
E: Assembly plant (PP)
F: Assembly year (Y)
G: Assembly week (WW)
H: Second level interconnect
I: Standard STMicroelectronics logo
J: Diffusion traceability plant (WX)
K: Dot(1)

1. *The dot on the back side indicates the pin 1 location.*

7 Ordering information

Table 7. **Ordering information**

Product family	Ordering code	Package	Factory firmware version	Supported interface(s)	A marking area	B marking area
ST33KTPM2XSPI	ST33KTPM2X32CKE2	UFQFPN32	9.256	SPI	KTPM	KE2
ST33KTPM2XI2C	ST33KTPM2X32CKE3	UFQFPN32	9.256	I²C & SPI	KTPM	KE3

8 Support and information

Additional information regarding ST TPM devices can be obtained from the www.st.com website.

For any specific support information you can contact STMicroelectronics through the following e-mail: *TPMsupport@list.st.com*.

STMicroelectronics has put in place a Product Security Incident Response Team (ST PSIRT). We encourage you to report any potential security vulnerability that you might suspect in our products through the ST PSIRT web page: https://www.st.com/psirt.

Revision history

Table 8. **Document revision history**

Date	Revision	Changes
10-May-2022	1	Initial release.
27-Jan-2023	2	Updated: • TPM features and Hardware features in cover page • Section 1 Description • Section 2 UFQFPN32 pin and signal description including Figure 1. UFQFPN32 pinout and Table 1. UFQFPN32 descriptions • Section 3.1 Recommended power supply filtering including Figure 2. Recommended filtering capacitors on V_{CC} and Table 2. V_{CC} rising slope • Section 3.2 SPI_CS optional filtering • Section 3.3 Device integration for SPI communication inlcuding Figure 3. Typical hardware implementation for SPI communication (UFQFPN32 package) • Section 3.4 Device integration for I²C communication including Figure 4. Typical hardware implementation for I²C communication (UFQFPN32 package) • Section 4.1 UFQFPN32 package information: corrected typo on introduction and on line D2 of Table 3. UFQFPN32 - Mechanical data

Glossary

AES Advanced encryption standard

CA Certification Authority

CC Common Criteria

DRBG Deterministic random bit generator

EC Elliptic curve

ECC Elliptic curve cryptography

ECDAA Elliptic curve direct anonymous attestation (algorithm)

ECDH Elliptic curve Diffie–Hellman

ECDSA Elliptic curve digital signature algorithm

EK Endorsement key

ESD Electrostatic discharge

FIPS Federal Information Processing Standards

GPIO General purpose input/output

HBM Human body model

HMAC Hash-based message authentication code or keyed-hash message authentication code

I²C Inter-integrated circuit

NIST National Institute of Standards and Technology

NV Nonvolatile

PKCS Public key cryptographic standards

PSS Probabilistic signature scheme

RNG Random number generator

RSA Public-key cryptosystem (created by Ron Rivest, Adi Shamir and Leonard Adleman)

RSAES Rivest Shamir Adelman encryption/decryption scheme

RSASSA Rivest Shamir Adelman signature scheme with appendix

SHA Secure Hash algorithm

SPI Serial peripheral interface

TCG Trusted Computing Group®

TPM Trusted platform module

TRNG True random number generator

TSS TPM software stack

Contents

List of tables

List of figures